US009479928B2

(12) **United States Patent**
Vats et al.

(10) **Patent No.: US 9,479,928 B2**
(45) **Date of Patent: Oct. 25, 2016**

(54) **CROSS-COMPONENT MESSAGE ENCRYPTION**

(75) Inventors: **Nikhil Vats**, Vaughn (CA); **Alexander Sherkin**, Woodbridge (CA); **Ravi Singh**, Toronto (CA); **Neil Patrick Adams**, Waterloo (CA); **Christopher Lyle Bender**, Kitchener (CA)

(73) Assignee: **BlackBerry Limited**, Waterloo (CA)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 420 days.

(21) Appl. No.: **13/296,501**

(22) Filed: **Nov. 15, 2011**

(65) **Prior Publication Data**

US 2012/0140927 A1 Jun. 7, 2012

Related U.S. Application Data

(60) Provisional application No. 61/413,941, filed on Nov. 15, 2010.

(51) **Int. Cl.**

H04L 29/06	(2006.01)
H04W 12/02	(2009.01)
H04L 9/32	(2006.01)

(Continued)

(52) **U.S. Cl.**

CPC ***H04W 12/02*** (2013.01); ***H04L 9/3247*** (2013.01); ***H04L 51/38*** (2013.01); ***H04L 63/0428*** (2013.01); *H04W 12/10* (2013.01)

(58) **Field of Classification Search**

CPC H04L 9/3247
USPC 380/270
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,764,899	A	6/1998	Eggleston et al.	
5,825,884	A *	10/1998	Zdepski	G06Q 20/0855 348/E7.056
6,134,582	A	10/2000	Kennedy	

(Continued)

FOREIGN PATENT DOCUMENTS

EP	2381998	A	5/2003
EP	1420554	A	5/2004

(Continued)

OTHER PUBLICATIONS

Examiner's Report, Nov. 27, 2013, Canadian Patent Application No. 2,758,429.

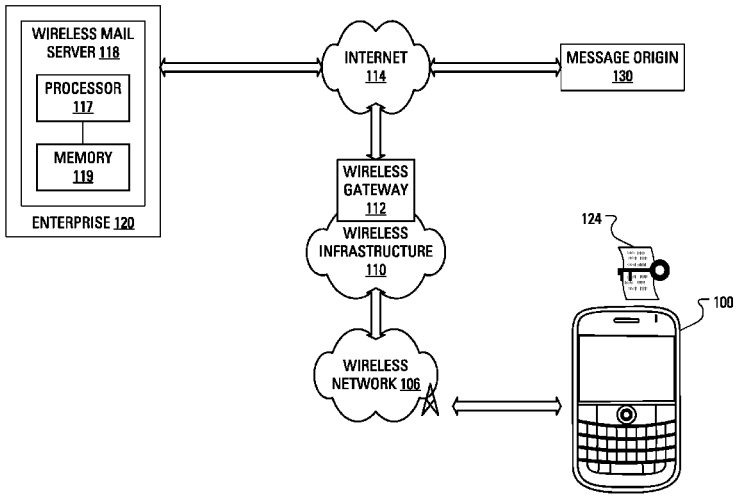
(Continued)

Primary Examiner — Hadi Armouche
Assistant Examiner — Ali Shayanfar
(74) *Attorney, Agent, or Firm* — Ridout & Maybee LLP

(57) **ABSTRACT**

Often, for reasons of wireless bandwidth conservation, incomplete messages are provided to wireless messaging devices. Employing cryptography, for secrecy or authentication purposes, when including a received message that has been incompletely received can lead to lack of context on the receiver's end. By automatically obtaining the entirety of the message to be included, an outgoing message that includes the received message can be processed in a manner that securely and accurately represents the intended outgoing message. Alternatively, a server can assemble a composite message from a new message and an original message and, in cooperation with a wireless messaging device, encrypt and sign the composite message. Conveniently, security considerations are maintained even in view of bandwidth optimization measures.

24 Claims, 13 Drawing Sheets



(51) **Int. Cl.**
H04L 12/58 (2006.01)
H04W 12/10 (2009.01)

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,289,105	B1	9/2001	Murota	
6,336,186	B1 *	1/2002	Dyksterhouse et al.	713/156
7,533,269	B2 *	5/2009	Kumagai et al.	713/176
8,423,772	B2 *	4/2013	Lee	H04L 63/083 380/270
8,538,022	B2 *	9/2013	Tu et al.	380/270
8,924,553	B2 *	12/2014	Schneider	H04L 9/3297 709/203
2003/0220978	A1 *	11/2003	Rhodes	H04L 12/585 709/206
2004/0090457	A1 *	5/2004	Serdy et al.	345/752
2004/0186990	A1	9/2004	Lai et al.	
2004/0205330	A1	10/2004	Godfrey et al.	
2005/0254658	A1 *	11/2005	Brown et al.	380/286
2006/0031299	A1	2/2006	Robertson	
2006/0031327	A1 *	2/2006	Kredo	709/206
2006/0036865	A1	2/2006	Brown et al.	
2006/0085509	A1	4/2006	Wener	
2007/0005713	A1 *	1/2007	LeVasseur et al.	709/206
2007/0162518	A1 *	7/2007	Tian	707/201
2007/0168436	A1 *	7/2007	Andam	709/206
2009/0034729	A1 *	2/2009	Brown et al.	380/270
2009/0080661	A1 *	3/2009	Brown et al.	380/279
2009/0097657	A1 *	4/2009	Scheidt et al.	380/277
2009/0307302	A1 *	12/2009	Tennant	H04L 67/1095 709/203
2009/0327714	A1 *	12/2009	Yaghmour	713/168
2010/0232606	A1 *	9/2010	Lee	H04L 63/08 380/270
2010/0250607	A1 *	9/2010	Noh	G06Q 10/00 707/783
2011/0055552	A1 *	3/2011	Francis	H04L 63/0421 713/153
2011/0076987	A1 *	3/2011	Lee	H04W 60/04 455/411
2012/0128156	A1 *	5/2012	Sherkin	H04L 12/58 380/270

FOREIGN PATENT DOCUMENTS

EP	1919084	A1	5/2008
EP	2020789		2/2009
EP	2020789	A1	2/2009
WO	2005107140	A1	11/2005

OTHER PUBLICATIONS

Extended European Search Report relating to application No. 09161927.0, dated Nov. 8, 2010.

Murphy, Galvin S. et al. "Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted; rfc1847.txt". Oct. 1995, IETF Standard, Internet Engineering Task Force, IETF, CH XP015007632. ISSN: 0000-0003.

Canadian Examiner's Report, Dated Feb. 26, 2015, U.S. Appl. No. 2,758,429.

* cited by examiner

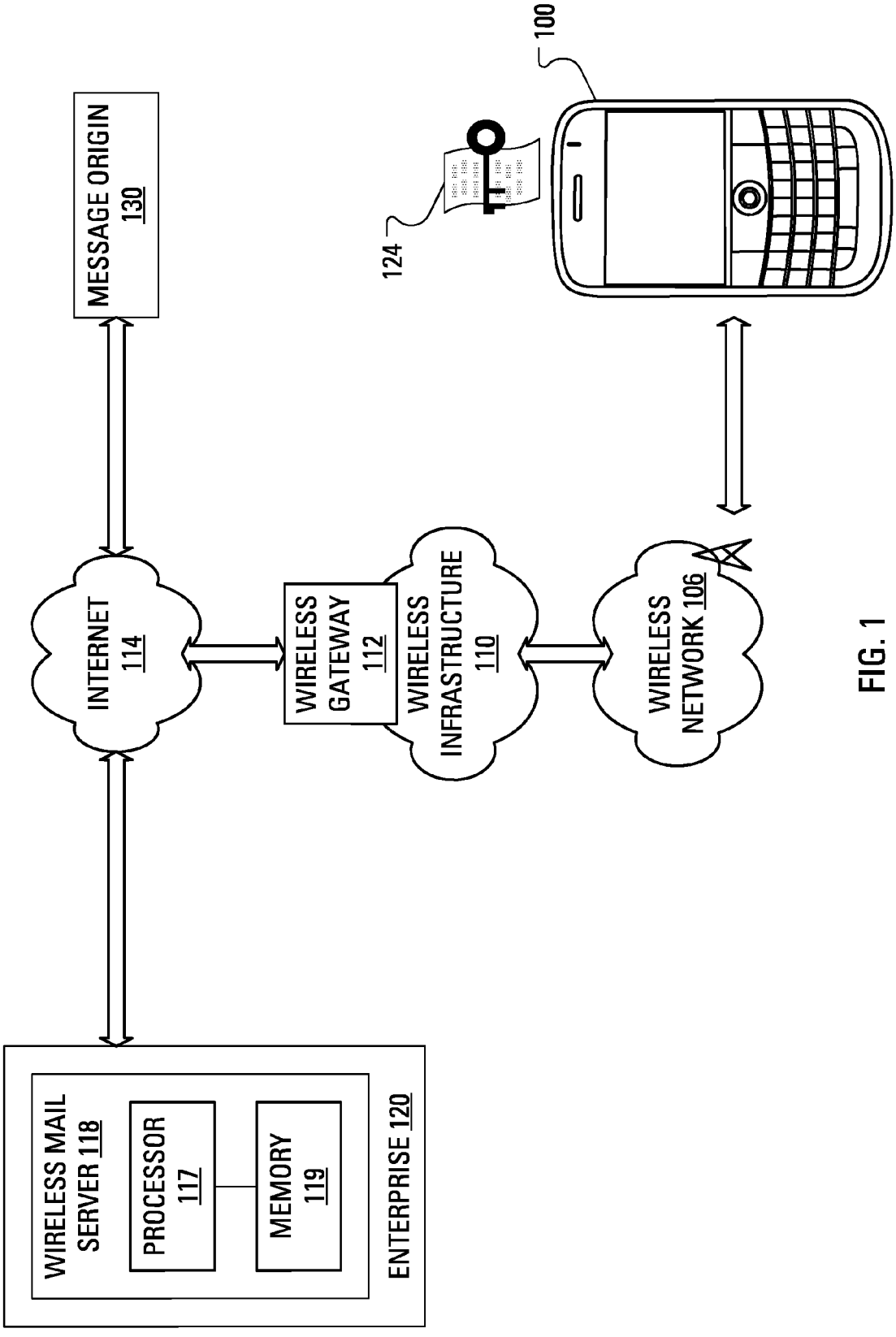

100
124
MESSAGE ORIGIN 130
INTERNET 114
WIRELESS GATEWAY 112
WIRELESS INFRASTRUCTURE 110
WIRELESS NETWORK 106
WIRELESS MAIL SERVER 118
PROCESSOR 117
MEMORY 119
ENTERPRISE 120

FIG. 1

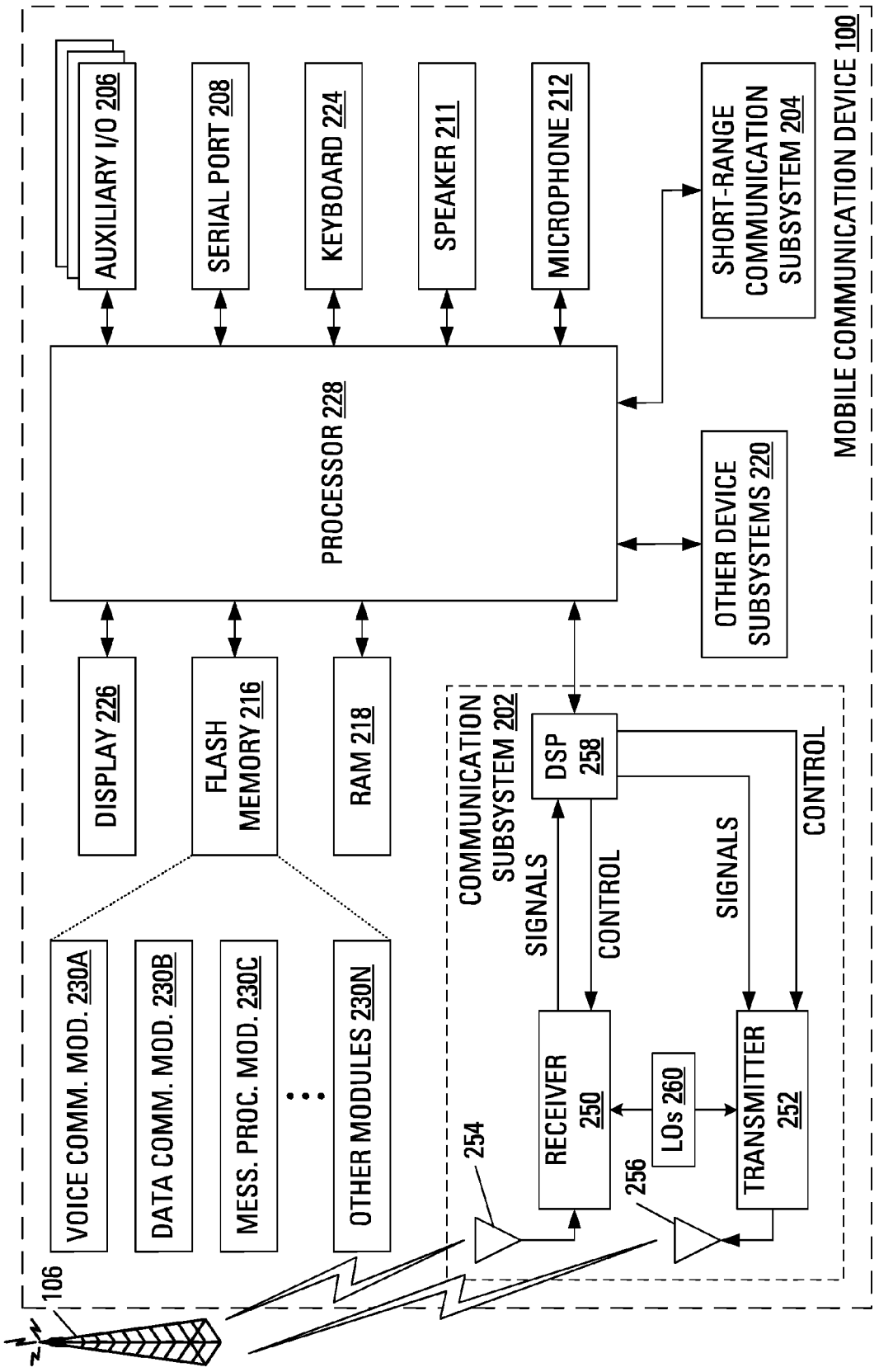

MOBILE COMMUNICATION DEVICE 100
AUXILIARY I/O 206
SERIAL PORT 208
KEYBOARD 224
SPEAKER 211
MICROPHONE 212
SHORT-RANGE COMMUNICATION SUBSYSTEM 204
PROCESSOR 228
OTHER DEVICE SUBSYSTEMS 220
DISPLAY 226
FLASH MEMORY 216
RAM 218
COMMUNICATION SUBSYSTEM 202
DSP 258
SIGNALS
CONTROL
SIGNALS
CONTROL
VOICE COMM. MOD. 230A
DATA COMM. MOD. 230B
MESS. PROC. MOD. 230C
OTHER MODULES 230N
RECEIVER 250
LOs 260
TRANSMITTER 252
254
256
106

FIG. 2

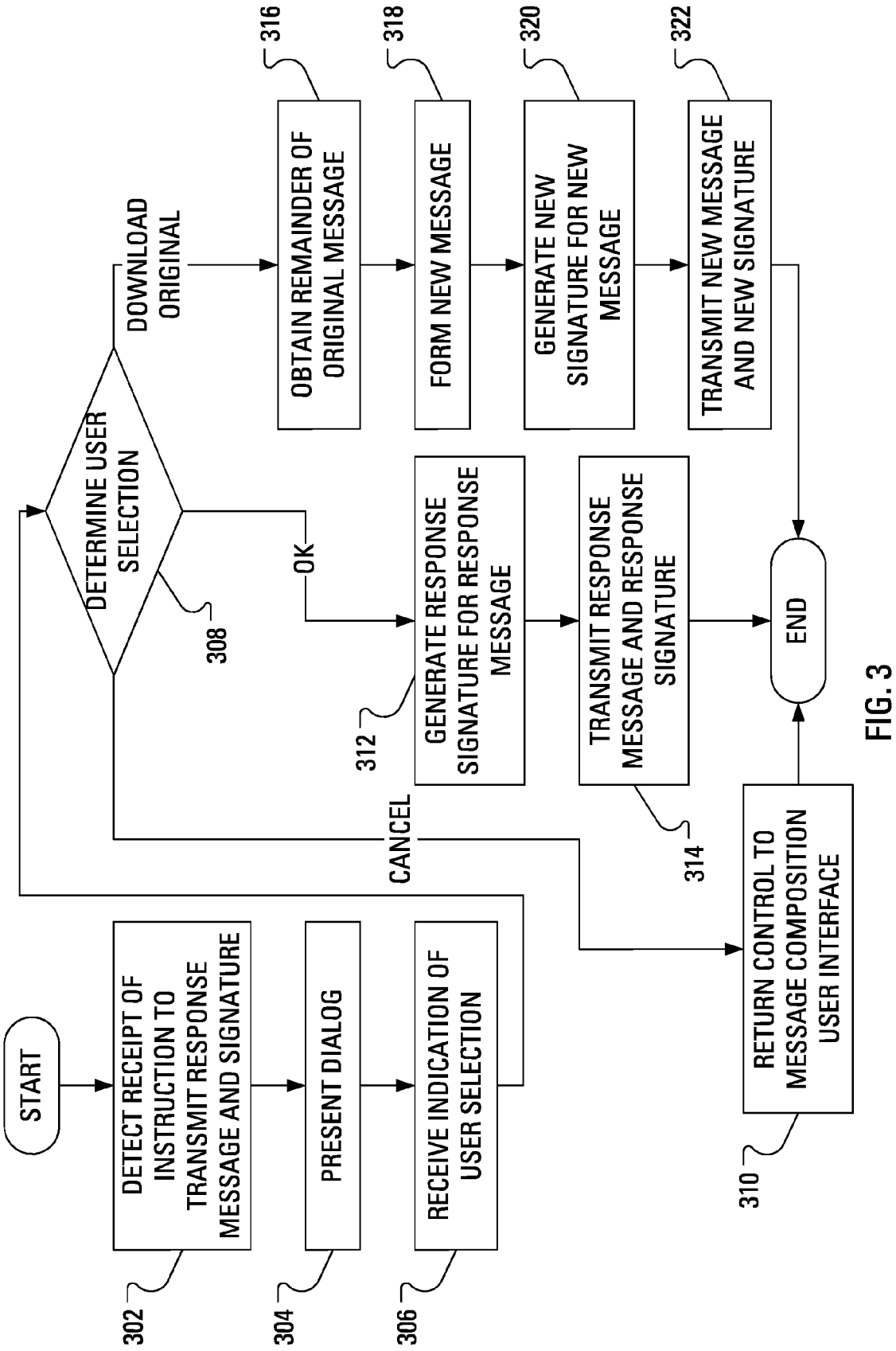

START
DETECT RECEIPT OF INSTRUCTION TO TRANSMIT RESPONSE MESSAGE AND SIGNATURE
302
PRESENT DIALOG
304
RECEIVE INDICATION OF USER SELECTION
306
DETERMINE USER SELECTION
308
DOWNLOAD ORIGINAL
OBTAIN REMAINDER OF ORIGINAL MESSAGE
316
FORM NEW MESSAGE
318
GENERATE NEW SIGNATURE FOR NEW MESSAGE
320
TRANSMIT NEW MESSAGE AND NEW SIGNATURE
322
OK
GENERATE RESPONSE SIGNATURE FOR RESPONSE MESSAGE
312
TRANSMIT RESPONSE MESSAGE AND RESPONSE SIGNATURE
314
CANCEL
END
RETURN CONTROL TO MESSAGE COMPOSITION USER INTERFACE
310

FIG. 3

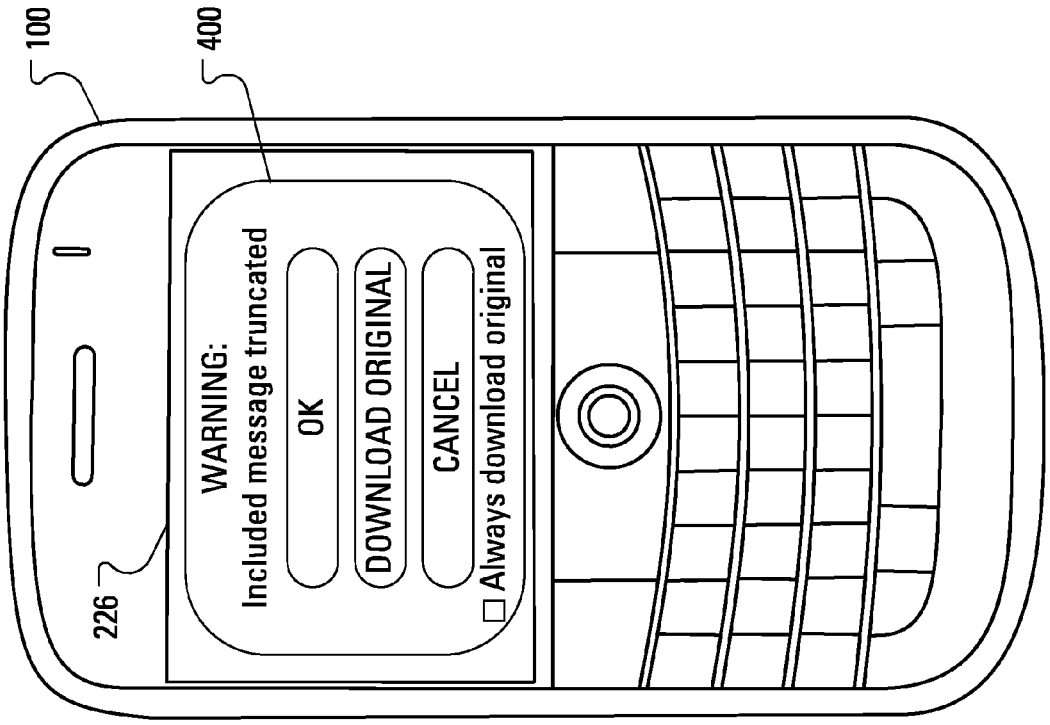

100
400
226
WARNING:
Included message truncated
OK
DOWNLOAD ORIGINAL
CANCEL
Always download original

FIG. 4

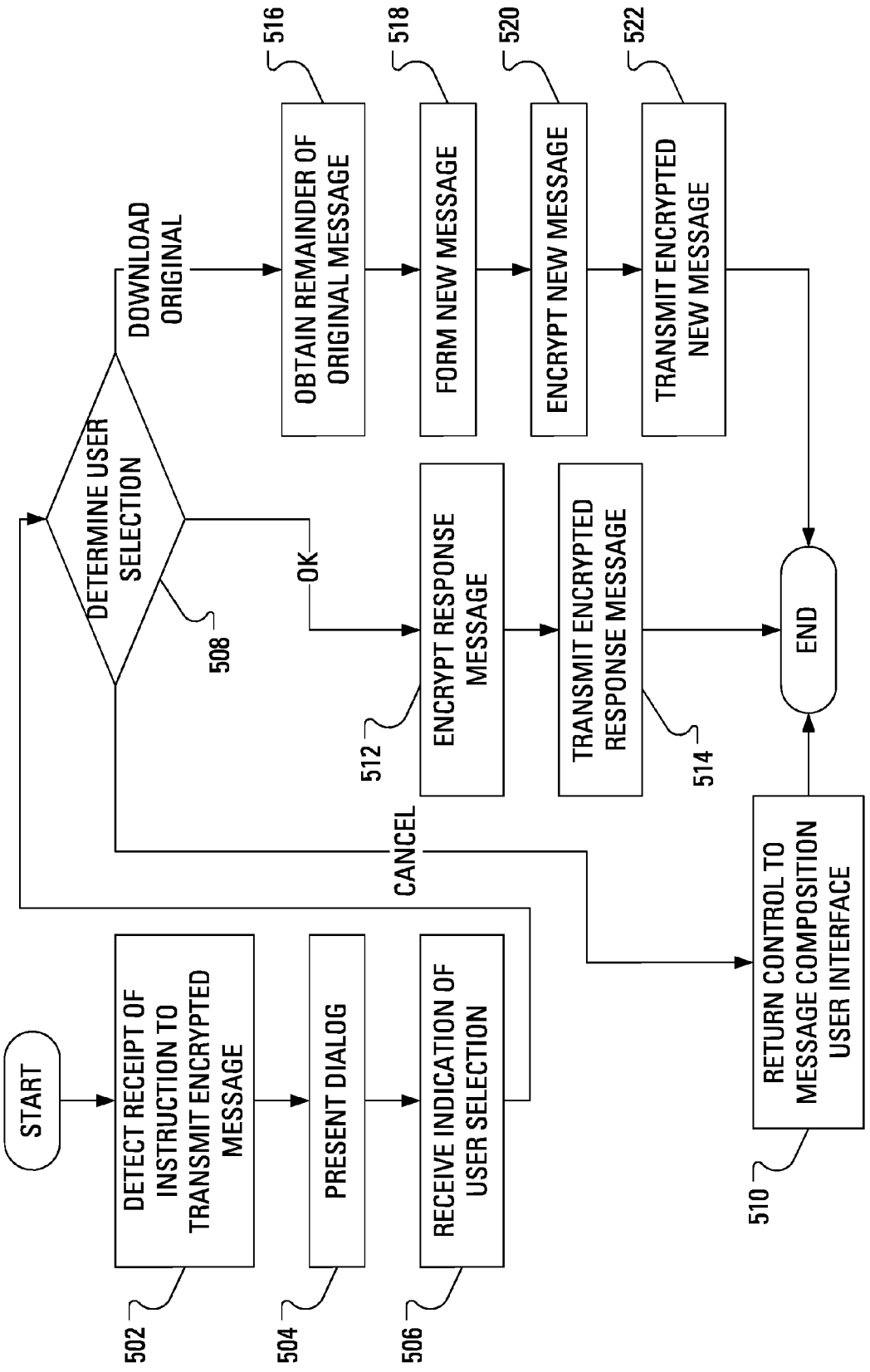

START
DETECT RECEIPT OF INSTRUCTION TO TRANSMIT ENCRYPTED MESSAGE
PRESENT DIALOG
RECEIVE INDICATION OF USER SELECTION
DETERMINE USER SELECTION
DOWNLOAD ORIGINAL
OBTAIN REMAINDER OF ORIGINAL MESSAGE
FORM NEW MESSAGE
ENCRYPT NEW MESSAGE
TRANSMIT ENCRYPTED NEW MESSAGE
OK
ENCRYPT RESPONSE MESSAGE
TRANSMIT ENCRYPTED RESPONSE MESSAGE
CANCEL
RETURN CONTROL TO MESSAGE COMPOSITION USER INTERFACE
END
502
504
506
508
510
512
514
516
518
520
522

FIG. 5

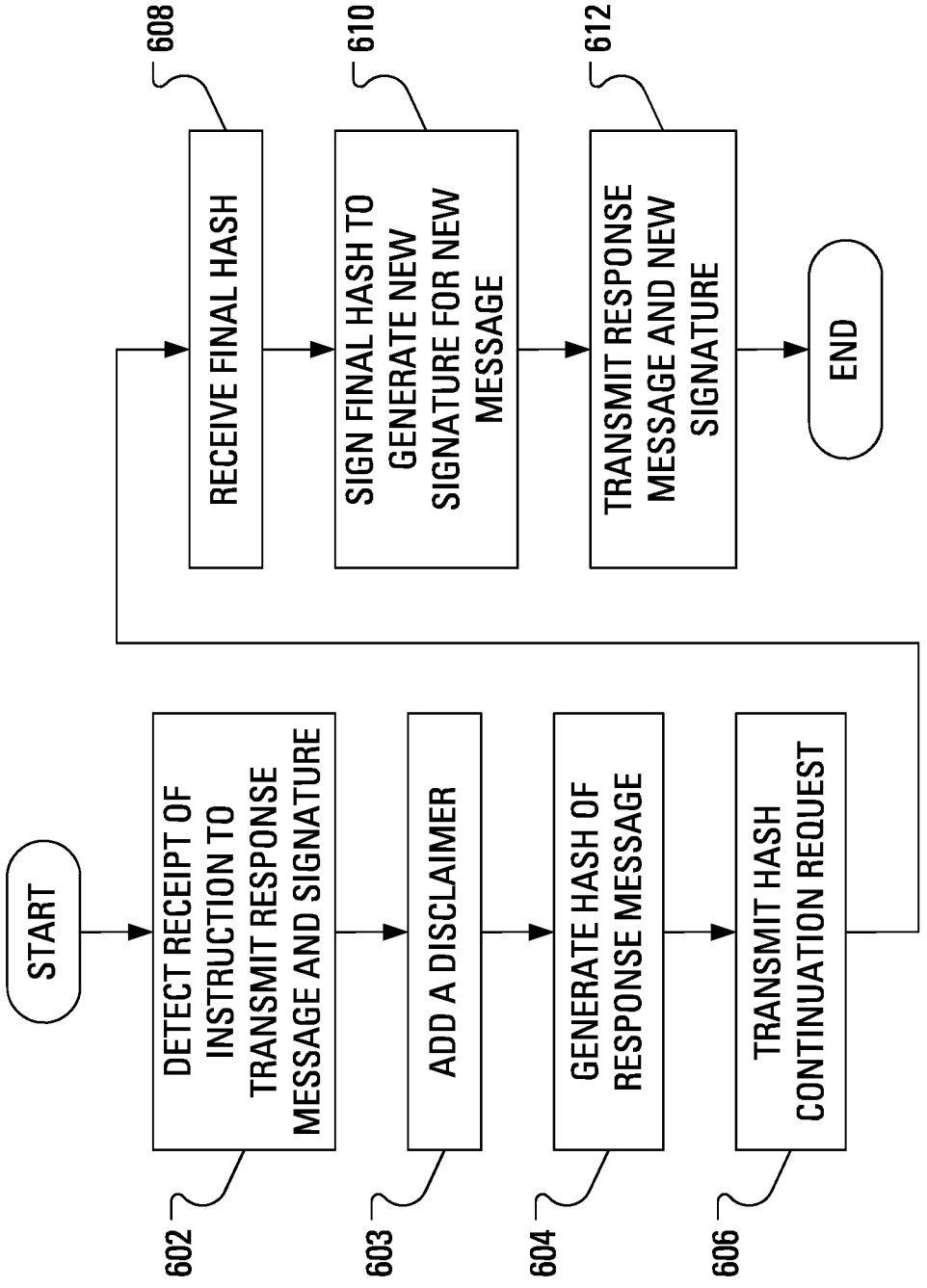

START
DETECT RECEIPT OF INSTRUCTION TO TRANSMIT RESPONSE MESSAGE AND SIGNATURE
602
ADD A DISCLAIMER
603
GENERATE HASH OF RESPONSE MESSAGE
604
TRANSMIT HASH CONTINUATION REQUEST
606
RECEIVE FINAL HASH
608
SIGN FINAL HASH TO GENERATE NEW SIGNATURE FOR NEW MESSAGE
610
TRANSMIT RESPONSE MESSAGE AND NEW SIGNATURE
612
END

FIG. 6

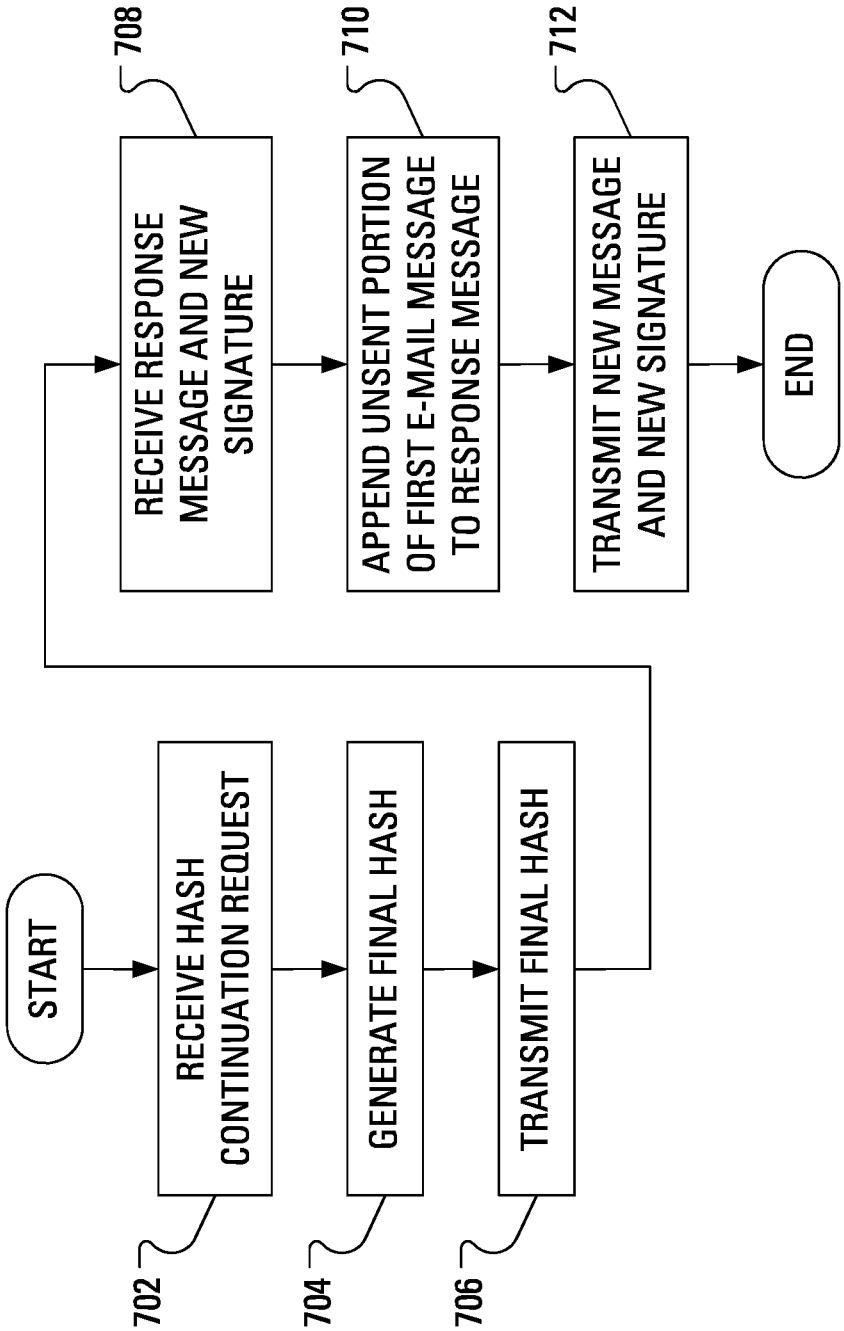

START
RECEIVE HASH CONTINUATION REQUEST
GENERATE FINAL HASH
TRANSMIT FINAL HASH
RECEIVE RESPONSE MESSAGE AND NEW SIGNATURE
APPEND UNSENT PORTION OF FIRST E-MAIL MESSAGE TO RESPONSE MESSAGE
TRANSMIT NEW MESSAGE AND NEW SIGNATURE
END
702
704
706
708
710
712

FIG. 7

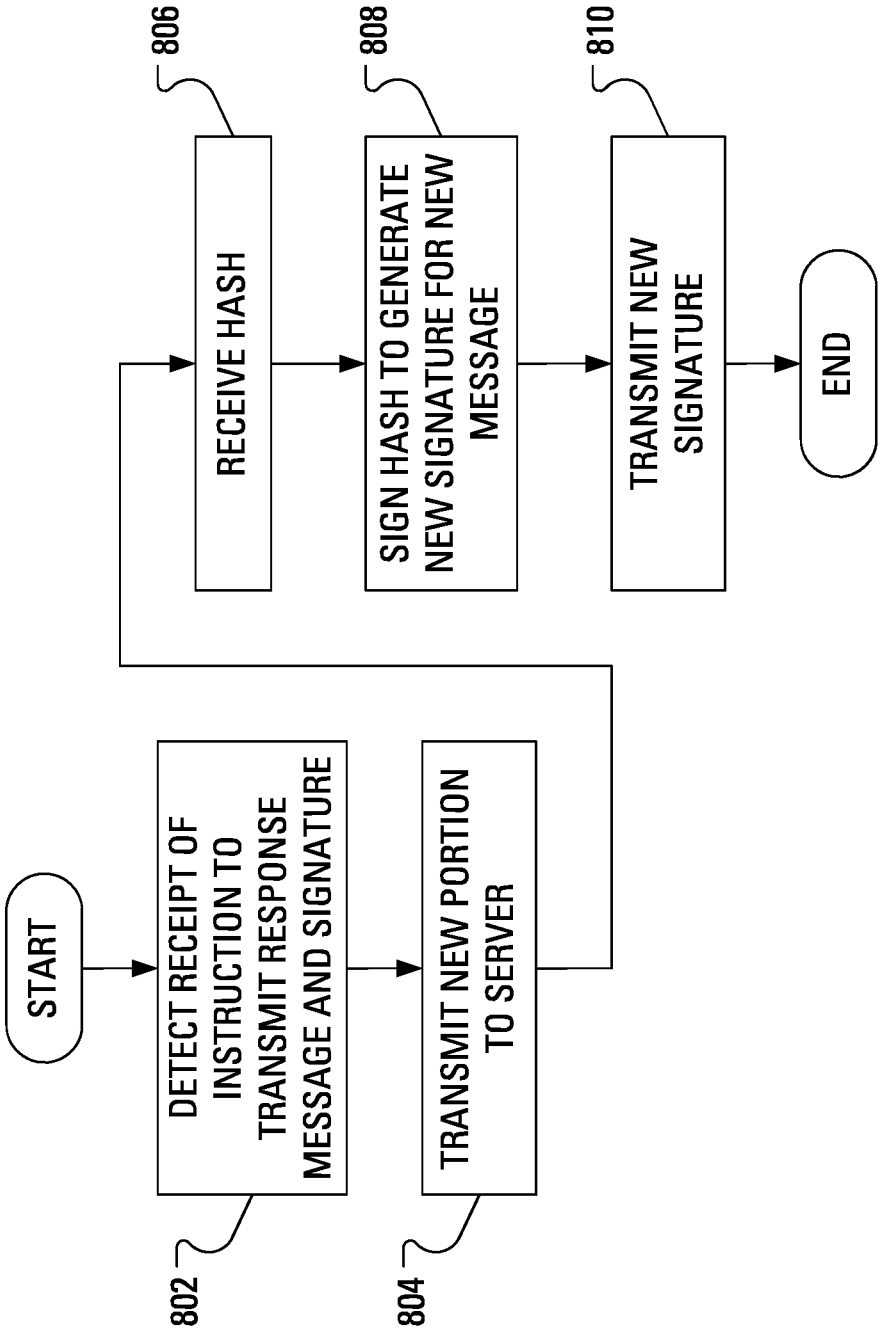

START
DETECT RECEIPT OF INSTRUCTION TO TRANSMIT RESPONSE MESSAGE AND SIGNATURE
802
TRANSMIT NEW PORTION TO SERVER
804
RECEIVE HASH
806
SIGN HASH TO GENERATE NEW SIGNATURE FOR NEW MESSAGE
808
TRANSMIT NEW SIGNATURE
810
END

FIG. 8

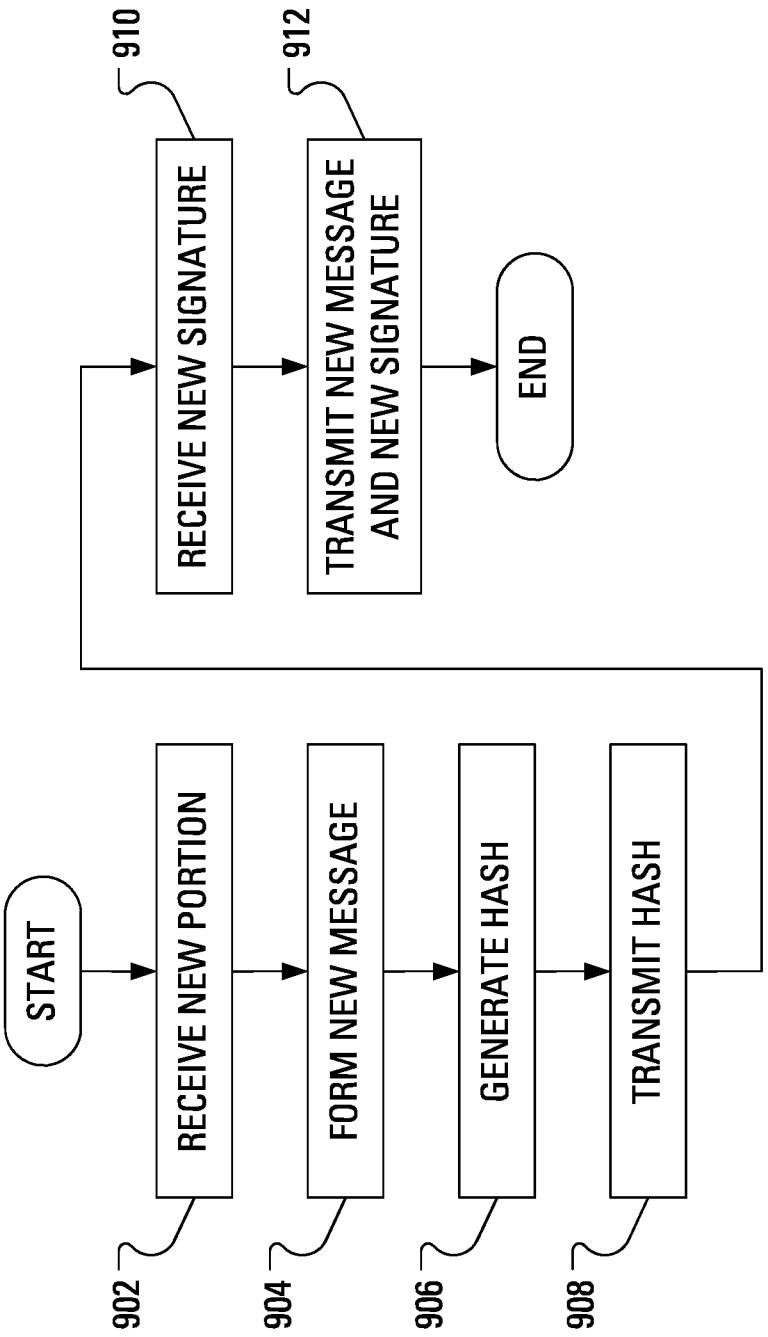

START
RECEIVE NEW PORTION
FORM NEW MESSAGE
GENERATE HASH
TRANSMIT HASH
RECEIVE NEW SIGNATURE
TRANSMIT NEW MESSAGE AND NEW SIGNATURE
END
902
904
906
908
910
912

FIG. 9

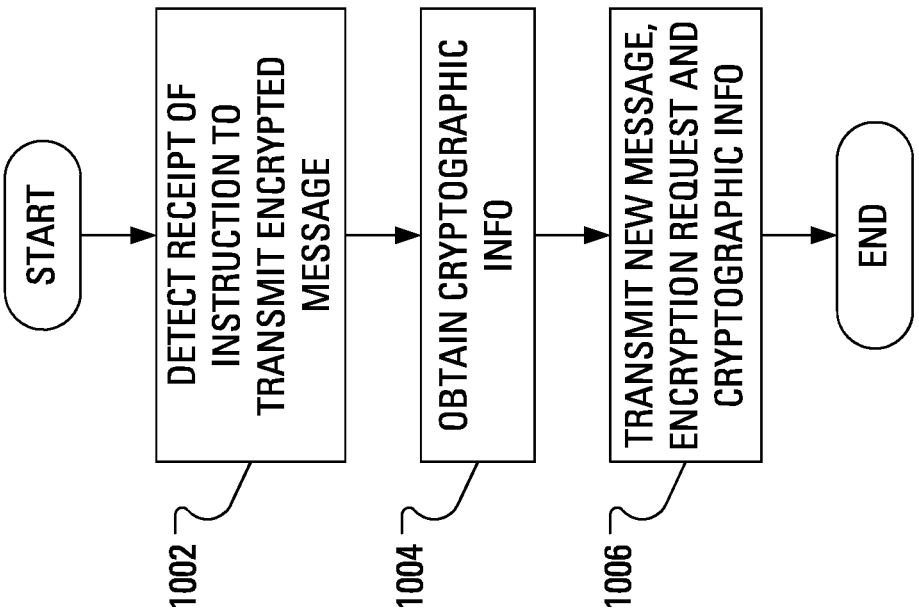

START
DETECT RECEIPT OF INSTRUCTION TO TRANSMIT ENCRYPTED MESSAGE
OBTAIN CRYPTOGRAPHIC INFO
TRANSMIT NEW MESSAGE, ENCRYPTION REQUEST AND CRYPTOGRAPHIC INFO
END
1002
1004
1006

FIG. 10

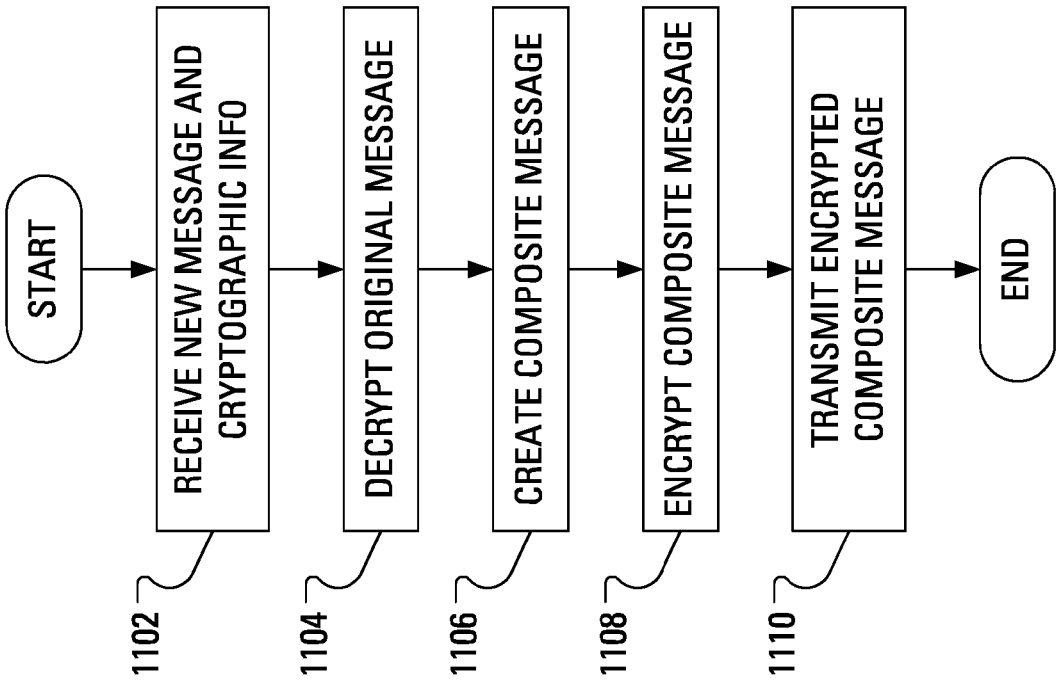

START
RECEIVE NEW MESSAGE AND CRYPTOGRAPHIC INFO
DECRYPT ORIGINAL MESSAGE
CREATE COMPOSITE MESSAGE
ENCRYPT COMPOSITE MESSAGE
TRANSMIT ENCRYPTED COMPOSITE MESSAGE
END
1102
1104
1106
1108
1110

FIG. 11

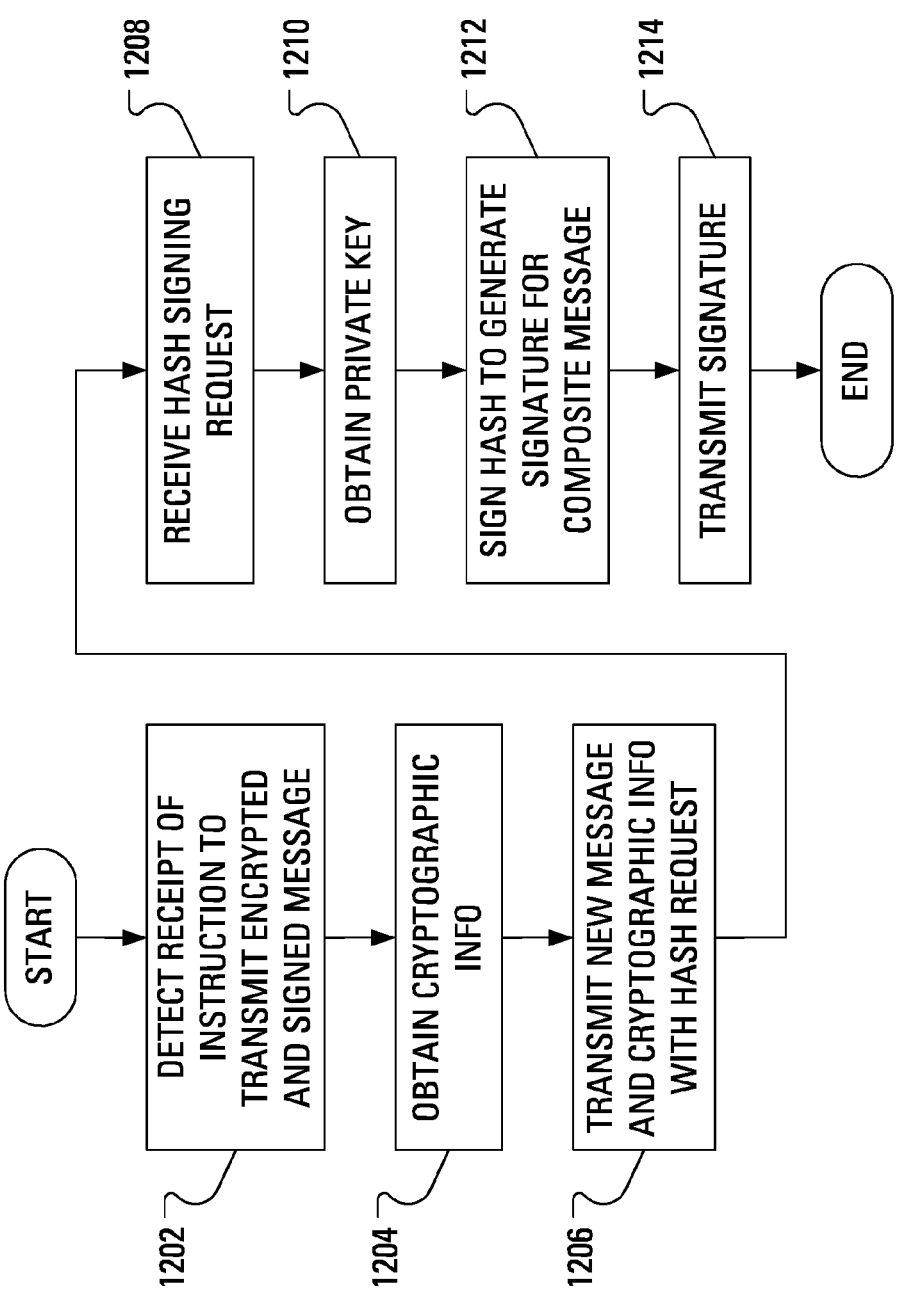

START
DETECT RECEIPT OF INSTRUCTION TO TRANSMIT ENCRYPTED AND SIGNED MESSAGE
OBTAIN CRYPTOGRAPHIC INFO
TRANSMIT NEW MESSAGE AND CRYPTOGRAPHIC INFO WITH HASH REQUEST
RECEIVE HASH SIGNING REQUEST
OBTAIN PRIVATE KEY
SIGN HASH TO GENERATE SIGNATURE FOR COMPOSITE MESSAGE
TRANSMIT SIGNATURE
END
1202
1204
1206
1208
1210
1212
1214

FIG. 12

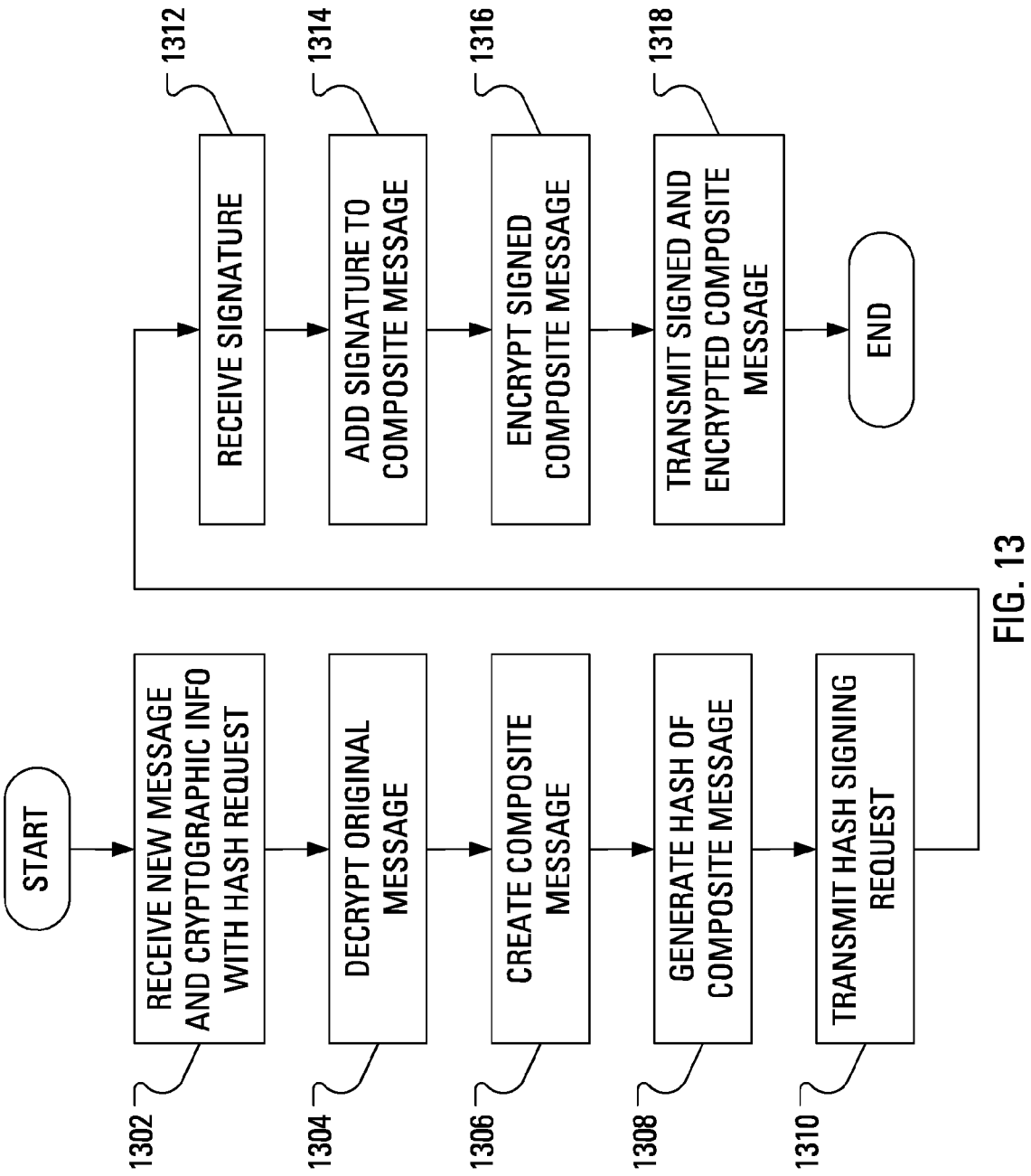

START
RECEIVE NEW MESSAGE AND CRYPTOGRAPHIC INFO WITH HASH REQUEST
1302
DECRYPT ORIGINAL MESSAGE
1304
CREATE COMPOSITE MESSAGE
1306
GENERATE HASH OF COMPOSITE MESSAGE
1308
TRANSMIT HASH SIGNING REQUEST
1310
RECEIVE SIGNATURE
1312
ADD SIGNATURE TO COMPOSITE MESSAGE
1314
ENCRYPT SIGNED COMPOSITE MESSAGE
1316
TRANSMIT SIGNED AND ENCRYPTED COMPOSITE MESSAGE
1318
END

FIG. 13

CROSS-COMPONENT MESSAGE ENCRYPTION

CROSS-REFERENCE TO RELATED APPLICATIONS

The present application claims priority from U.S. Provisional Patent Application Ser. No. 61/413,941, filed Nov. 15, 2010, the contents of which are hereby incorporated herein by reference.

FIELD

The present application relates generally to mobile wireless electronic messaging and, more specifically, to encrypting a message with the involvement of more than one component.

BACKGROUND

In one manner of processing (e.g., encrypting) an outgoing e-mail message, a communication application, employed by a given user, transforms the outgoing e-mail message using an algorithm with a public key half of a public-private key pair. The encrypted outgoing e-mail message may then be transmitted. Upon receiving the encrypted e-mail message, the recipient device may be configured to decrypt the received e-mail using a private key half of the public-private key pair.

BRIEF DESCRIPTION OF THE DRAWINGS

Reference will now be made to the drawings, which show by way of example, embodiments of the present application, and in which:

FIG. **1** illustrates an overview of an example system including a mobile communication device and a wireless mail server;

FIG. **2** illustrates a schematic representation of components of the mobile communication device of FIG. **1**;

FIG. **3** illustrates example steps in a first method of processing an electronic message at the mobile communication device of FIG. **1**, where the processing comprises signing;

FIG. **4** illustrates an example dialog to warn a user that an e-mail message will be incompletely included in a response message;

FIG. **5** illustrates example steps in the method of FIG. **3**, where the processing comprises encrypting;

FIG. **6** illustrates example steps in a second method of processing an electronic message at the mobile communication device of FIG. **1**, where the processing comprises signing;

FIG. **7** illustrates example steps in a method of processing an electronic message at the wireless mail server of FIG. **1**, in conjunction with the method of FIG. **6**;

FIG. **8** illustrates example steps in a third method of processing an electronic message at the mobile communication device of FIG. **1**, where the processing comprises signing;

FIG. **9** illustrates example steps in a method of processing an electronic message at the wireless mail server of FIG. **1**, in conjunction with the method of FIG. **8**;

FIG. **10** illustrates example steps of a cross-component message encryption approach;

FIG. **11** illustrates example steps in a method of participating, at the wireless mail server of FIG. **1**, in the cross-component message encryption approach of FIG. **10**;

FIG. **12** illustrates example steps of cross-component message encryption approach distinct from the cross-component message encryption approach of FIGS. **10** and **11**; and

FIG. **13** illustrates example steps in a method of participating, at the wireless mail server of FIG. **1**, in the cross-component message encryption approach of FIG. **12**.

DETAILED DESCRIPTION OF THE EMBODIMENTS

When a mobile wireless device is used to receive and transmit e-mail, the mobile wireless device is often associated with a mobile mail server. The mobile mail server manages the transmission of messages to the mobile wireless device to optimize use of the limited resources of a wireless communication channel in the path between the mobile wireless device and the mobile mail server. The mobile mail server may also manage messages transmitted by the mobile wireless device to optimize in a similar fashion.

For a first example of optimization of transmission of messages to the mobile wireless device, by only transmitting an initial portion of a first e-mail message to the mobile wireless device, the mobile mail server may conserve wireless resources that would otherwise be consumed by transmitting the entire first e-mail message.

It is common, in e-mail communication applications, to include the text of a received e-mail message when composing an e-mail message in response or when forwarding the e-mail message to a further recipient. However, in a mobile communication system, when sending a new e-mail message related to an original e-mail message, the mobile wireless device may only be able to include the initial portion of the original e-mail message in the new e-mail message, since the mobile wireless device may only have the initial portion of the original e-mail message available. Upon receiving the new e-mail message, the cleverly designed mobile mail server may append the remaining (i.e., non-initial) portion of the original e-mail message before forwarding the entire new e-mail message toward its destination. Conveniently, this scheme conserves wireless communication channel resources.

However, when a user of the mobile wireless device wishes to sign the new e-mail message, obtaining the efficiency of previously described schemes becomes challenging.

For example, consider receipt, at the mobile wireless device, of an initial portion of a first e-mail message. The user of the mobile wireless device reviews the initial portion of the first e-mail message and composes a response to the first e-mail message. The response may be considered a second e-mail message. The second e-mail message may be considered to have at least two portions: an "old" portion, comprising the initial portion of the first e-mail message; and a "new" portion, comprising the content composed by the user of the mobile wireless device. The user of the mobile wireless device may decide to sign the second e-mail message. Accordingly, when obtaining a signature to associate with the second e-mail message, the mobile wireless device may only obtain a hash of the second e-mail message (i.e., the old portion appended to the new portion). That is, the mobile wireless device encrypts a hash of the second e-mail message with the private key stored at the mobile

wireless device. The mobile mail server would normally append the remaining (i.e., non-initial) portion of the first e-mail message to the received second e-mail message to form a complete response, before forwarding the complete response to the origin of the first e-mail message. However, since the signature received in association with the second e-mail message only relates to the old portion appended to the new portion, and not to the complete response, the mobile mail server must simply forward the second e-mail message and associated signature toward the origin of the first e-mail message.

At the origin of the first e-mail message, the recipient of the second e-mail message does not receive all of the typically appended first e-mail message content and, accordingly, may struggle with the placing of the second e-mail message properly in context.

To provide awareness to the sender of the second e-mail message (i.e., the user of the mobile wireless device) that the second e-mail message will include only a truncated version of the first e-mail message, the mobile wireless device may display a warning dialog. The warning dialog may be displayed responsive to the user of the mobile wireless device indicating, using a user interface in a message composition mode, that the second e-mail message is to be sent. The warning dialog may indicate "Warning! Your message will be truncated." Furthermore, the warning dialog may be interactive and may require user selection of a choice before the warning dialog may be dismissed from the display. That is, the warning dialog may present choices labeled "OK" and "Cancel". Additionally, the warning dialog may include a checkbox labeled "Don't show this dialog again". The user may select the "OK" choice to indicate acceptance of the truncation. Alternatively, the user may select the "Cancel" choice to indicate a wish to return to composing the message. By selecting the checkbox labeled "Don't show this dialog again" and then selecting the "OK" choice, the user may effectively set a policy for the mobile wireless device, where the policy indicates that all future signed, and/or encrypted, messages are to include only a truncated version of the original received message.

Upon receiving an indication that the user has selected the "OK" choice, the mobile wireless device may proceed to transmit the second e-mail message to the mobile mail server for forwarding to the sender of the first e-mail message.

Upon receiving an indication that the user has selected the "Cancel" choice, the mobile wireless device may return the user interface to the message composition mode. Responsive to being returned to the message composition mode, the user may manipulate the user interface to copy, to a clipboard, the message that has been typed (i.e., the new portion). The user may then close the message composition user interface, return to a message list and re-open the first message. Once the initial portion of the first message is open, the user may manipulate a message viewing user interface to request, from the mobile mail server, the entire first message. The user may then manipulate the message viewing user interface to indicate a wish to compose a response to the first message. Once the message composition user interface has been opened, pre-loaded with the entirety of the first e-mail message, the user may paste the previously composed new portion from the clipboard to the message composition area in the message composition user interface, thereby creating a third e-mail message. The third e-mail message may be distinguished from the second e-mail message in that the third e-mail message includes the entirety of the first e-mail message and the second e-mail message only includes a truncated version of the first e-mail message. The user may then create a signature for the third e-mail message and indicate that the third e-mail message and the signature are to be sent.

One can see that including an entire original message in a signed response can require manually carrying out some potentially tedious and complex steps.

By arranging assembly, at a server, of a composite message from a new message and an original message and arranging encryption and signing of the composite message in cooperation with a wireless messaging device, operational complexity on the part of the user can be obviated.

In an aspect of the present disclosure there is provided a method of processing an electronic message at a mobile wireless communication device. The method includes detecting receipt of an instruction to encrypt and transmit a composite message, where the composite message includes a new message and an original message, obtaining cryptographic information for use in carrying out the encryption request, transmitting the new message to a server associated with the mobile wireless communication device and transmitting an encryption request to the server, the encryption request including the cryptographic information and specifying the original message. In other aspects of the present application, a mobile wireless communication device is provided for carrying out this method and a computer readable medium is provided for adapting a processor to carry out this method.

In another aspect of the present disclosure there is provided a method of processing an electronic message. The method includes detecting receipt of a message processing request for encryption and transmission of a composite message, where the composite message includes a new message and an original message, the message processing request including the new message, an indication of the original message and cryptographic information for use in the encryption, creating the composite message from the new message and the original message, employing a first portion of the cryptographic information to encrypt the composite message to form an encrypted composite message and transmitting the encrypted composite message. In other aspects of the present application, a mail server is provided for carrying out this method and a computer readable medium is provided for adapting a processor to carry out this method.

Other aspects and features of the present application will become apparent to those of ordinary skill in the art upon review of the following description of specific embodiments of the application in conjunction with the accompanying figures.

Referring to FIG. **1**, an overview of an example system for use with the embodiments described below is shown. One skilled in the art will appreciate that there may be many different topologies, but the system shown in FIG. **1** helps demonstrate the operation of the systems and methods described in the present application. For example, there may be many mobile communication devices connected to the system that are not shown in the overview of FIG. **1**.

FIG. **1** shows a mobile wireless device in the form of a mobile communication device **100**. It will be appreciated by those skilled in the art that the mobile communication device **100** may comprise any computing or communication device that is capable of connecting to a network by wireless means, including, but not limited, to personal computers (including tablet and laptop computers), personal digital assistants, smart phones, and the like. It will further be appreciated by those skilled in the art that these devices may

be referred to herein as computing devices or communication devices, and may have principal functions directed to data or voice communication over a network, data storage or data processing, or the operation of personal or productivity applications; those skilled in the art will appreciate that terminology such as "mobile device", "communication device", "computing device", or "user device" may be used interchangeably.

The mobile communication device **100** may, for example, be connected to an Internet Service Provider on which a user of the system of FIG. **1**, likely the user associated with the mobile communication device **100** illustrated in FIG. **1**, has an account.

The mobile communication device **100** may be capable of sending and receiving messages and other data via wireless transmission and reception, as is typically done using electromagnetic waves in the radio frequency (RF) spectrum. The exchange of messages and other data may occur, for instance, between the mobile communication device **100** and a base station in a wireless carrier network **106**. The mobile communication device **100** may receive data by other means, for example through a direct connection to a port provided on the mobile communication device **100**. An example of such a direct connection is a Universal Serial Bus (USB) link.

As illustrated in FIG. **1**, the wireless carrier network **106** connects to a wide area network **114**, represented as the Internet, via a wireless infrastructure **110**. The wireless infrastructure **110** incorporates a wireless gateway **112** for connecting to the Internet **114**.

A connection between the mobile communication device **100** and the Internet **114** allows the mobile communication device **100** to access a wireless mail server **118**. The wireless mail server **118** may include a processor **117** and a memory **119**. The wireless mail server **118** may be grouped together with other servers (not shown) in an enterprise **120**. Also connected to the Internet **114** may be a representative message origin **130**. The mobile communication device **100** may store a private cryptographic key **124** that is associated with a corresponding public cryptographic key.

FIG. **2** illustrates the mobile communication device **100**. The mobile communication device **100** includes a housing, an input device (e.g., a keyboard **224** having a plurality of keys) and an output device (e.g., a display **226**), which may be a full graphic, or full color, Liquid Crystal Display (LCD). In some embodiments, the display **226** may comprise a touchscreen display. In such embodiments, the keyboard **224** may comprise a virtual keyboard. Other types of output devices may alternatively be utilized. A processing device (a processor **228**) is shown schematically in FIG. **2** as coupled between the keyboard **224** and the display **226**. The processor **228** controls the operation of the display **226**, as well as the overall operation of the mobile communication device **100**, in part, responsive to actuation of the keys on the keyboard **224** by a user. Notably, the keyboard **224** may comprise physical buttons (keys) or, where the display **226** is a touchscreen device, the keyboard **224** may be implemented, at least in part, as "soft keys". Actuation of a so-called soft key involves either touching the display **226** where the soft key is displayed or actuating a physical button in proximity to an indication, on the display **226**, of a temporary action associated with the physical button.

The housing may be elongated vertically, or may take on other sizes and shapes (including clamshell housing structures). Where the keyboard **224** includes keys that are associated with at least one alphabetic character and at least one numeric character, the keyboard **224** may include a mode selection key, or other hardware or software, for switching between alphabetic entry and numeric entry.

In addition to the processor **228**, other parts of the mobile communication device **100** are shown schematically in FIG. **2**. These may include a communications subsystem **202**, a short-range communications subsystem **204**, the keyboard **224** and the display **226**. The mobile communication device **100** may further include other input/output devices, such as a set of auxiliary I/O devices **206**, a serial port **208**, a speaker **211** and a microphone **212**. The mobile communication device **100** may further include memory devices including a flash memory **216** and a Random Access Memory (RAM) **218** and various other device subsystems **220**. The mobile communication device **100** may comprise a two-way radio frequency (RF) communication device having voice and data communication capabilities. In addition, the mobile communication device **100** may have the capability to communicate with other computer systems via the Internet.

Operating system software executed by the processor **228** may be stored in a computer readable medium, such as the flash memory **216**, but may be stored in other types of memory devices, such as a read only memory (ROM) or similar storage element. In addition, system software, specific device applications, or parts thereof, may be temporarily loaded into a volatile store, such as the RAM **218**. Communication signals received by the mobile device may also be stored to the RAM **218**.

The processor **228**, in addition to its operating system functions, enables execution of software applications on the mobile communication device **100**. A predetermined set of software applications that control basic device operations, such as a voice communications module **230**A and a data communications module **230**B, may be installed on the mobile communication device **100** during manufacture. A message processing module **230**C may also be installed on the mobile communication device **100** during manufacture, to implement aspects of the present disclosure. As well, additional software modules, illustrated as an other software module **230**N, which may be, for instance, a PIM application, may be installed during manufacture. The PIM application may be capable of organizing and managing data items, such as e-mail messages, calendar events, voice mail messages, appointments and task items. The PIM application may also be capable of sending and receiving data items via a wireless carrier network **106** represented by a radio tower. The data items managed by the PIM application may be seamlessly integrated, synchronized and updated via the wireless carrier network **106** with the device user's corresponding data items stored or associated with a host computer system.

Communication functions, including data and voice communications, are performed through the communication subsystem **202** and, possibly, through the short-range communications subsystem **204**. The communication subsystem **202** includes a receiver **250**, a transmitter **252** and one or more antennas, illustrated as a receive antenna **254** and a transmit antenna **256**. In addition, the communication subsystem **202** also includes a processing module, such as a digital signal processor (DSP) **258**, and local oscillators (LOs) **260**. The specific design and implementation of the communication subsystem **202** is dependent upon the communication network in which the mobile communication device **100** is intended to operate. For example, the communication subsystem **202** of the mobile communication device **100** may be designed to operate with the Mobitex™, DataTAC™ or General Packet Radio Service (GPRS) mobile data communication networks and also designed to

operate with any of a variety of voice communication networks, such as Advanced Mobile Phone Service (AMPS), Time Division Multiple Access (TDMA), Code Division Multiple Access (CDMA), Personal Communications Service (PCS), Global System for Mobile Communications (GSM), Enhanced Data rates for GSM Evolution (EDGE), Universal Mobile Telecommunications System (UMTS), Wideband Code Division Multiple Access (W-CDMA), High Speed Packet Access (HSPA), etc. Other types of data and voice networks, both separate and integrated, may also be utilized with the mobile communication device **100**.

Network access requirements vary depending upon the type of communication system. Typically, an identifier is associated with each mobile device that uniquely identifies the mobile device or subscriber to which the mobile device has been assigned. The identifier is unique within a specific network or network technology. For example, in Mobitex™ networks, mobile devices are registered on the network using a Mobitex Access Number (MAN) associated with each device in DataTAC™ networks, mobile devices are registered on the network using a Logical Link Identifier (LLI) associated with each device. In GPRS networks, however, network access is associated with a subscriber or user of a device. A GPRS device therefore uses a subscriber identity module, commonly referred to as a Subscriber Identity Module (SIM) card, in order to operate on a GPRS network. Despite identifying a subscriber by SIM, mobile devices within GSM/GPRS networks are uniquely identified using an International Mobile Equipment Identity (IMEI) number.

When required network registration or activation procedures have been completed, the mobile communication device **100** may send and receive communication signals over the wireless carrier network **106**. Signals received from the wireless carrier network **106** by the receive antenna **254** are routed to the receiver **250**, which provides for signal amplification, frequency down conversion, filtering, channel selection, etc., and may also provide analog to digital conversion. Analog-to-digital conversion of the received signal allows the DSP **258** to perform more complex communication functions, such as demodulation and decoding. In a similar manner, signals to be transmitted to the wireless carrier network **106** are processed (e.g., modulated and encoded) by the DSP **258** and are then provided to the transmitter **252** for digital to analog conversion, frequency up conversion, filtering, amplification and transmission to the wireless carrier network **106** (or networks) via the transmit antenna **256**.

In addition to processing communication signals, the DSP **258** provides for control of the receiver **250** and the transmitter **252**. For example, gains applied to communication signals in the receiver **250** and the transmitter **252** may be adaptively controlled through automatic gain control algorithms implemented in the DSP **258**.

In a data communication mode, a received signal, such as a text message or web page download, is processed by the communication subsystem **202** and is input to the processor **228**. The received signal is then further processed by the processor **228** for output to the display **226**, or alternatively to some auxiliary I/O devices **206**. A device user may also compose data items, such as e-mail messages, using the keyboard **224** and/or some other auxiliary I/O device **206**, such as a touchpad, a rocker switch, a thumb-wheel, a trackball, a touchscreen, or some other type of input device. The composed data items may then be transmitted over the wireless carrier network **106** via the communication subsystem **202**.

In a voice communication mode, overall operation of the device is substantially similar to the data communication mode, except that received signals are output to the speaker **211**, and signals for transmission are generated by a microphone **212**. Alternative voice or audio I/O subsystems, such as a voice message recording subsystem, may also be implemented on the mobile communication device **100**. In addition, the display **226** may also be utilized in voice communication mode, for example, to display the identity of a calling party, the duration of a voice call, or other voice call related information.

The short-range communications subsystem **204** enables communication between the mobile communication device **100** and other proximate systems or devices, which need not necessarily be similar devices. For example, the short-range communications subsystem may include an infrared device and associated circuits and components, or a Bluetooth™ communication module to provide for communication with similarly-enabled systems and devices.

In overview, the mobile communication device **100** receives an initial portion of a first e-mail message from the wireless mail server **118**, where the first e-mail message has originated at the representative message origin **130**. The user of the mobile communication device **100** manipulates the mobile communication device **100** to invoke a message composition user interface preloaded with the received initial portion of the first e-mail message and composes a new portion. Where the user has specified that the message is to be processed (e.g., signed and/or encrypted), responsive to the user indicating that the message is to be sent, aspects of the present disclosure allow for the processing of a new message that includes the new portion and the entirety of the first e-mail message.

For example, the message composition user interface may allow the user to specify that the message is to be signed. Typically, when the user has indicated that the message is to be sent, the message composition user interface prompts the user for a password associated with a key store in which the private cryptographic key **124** is stored. Upon verifying a received password, the processor **228** executes a message signing algorithm to generate a signature by, first, generating a hash of the message and, second, encrypting the hash with the private cryptographic key **124**.

In a first cross-component message processing approach, some automation is provided to the complex operations. Responsive to the user indicating that a reply message with truncated original message is to be sent, it is proposed herein to prompt the user with a dialog that includes a user option to "Download Original". Responsive to receiving an indication that the "Download Original" user option has been selected, the processor **228** may automatically download the remainder of the original message and append the remainder of the original message to the reply message. The processor **228** may then sign, encrypt or sign and encrypt the reply message with the entire original message before sending, thereby providing full, end-to-end security.

Steps of a method that is an example of a first cross-component message signing approach are presented in FIG. **3**. Initially, the processor **228**, or, more accurately, a signature handling application executed on the processor **228**, detects receipt (step **302**) of an instruction to transmit a response message and an associated signature. Such an instruction may be received from the message composition user interface application also executed on the processor **228**.

From the user's perspective, the user has specified that the response message is to be signed and the user has composed

the new portion of the response message (in any order). The user may have configured the mobile communication device **100**, at some earlier time, to, by default, transmit an associated signature with each outgoing messages. The receipt (detected in step **302**), by the signature handling application, of the instruction to transmit a response message and an associated signature may be triggered by the user opening a menu and selecting a "send" menu item.

Responsive to the detection in step **302**, the signature handling application may present (step **304**) a dialog to warn the user that the first e-mail message will be incompletely included in the response message and giving the user choice regarding how or whether to proceed. An example of a suitable dialog is illustrated as a dialog **400** in FIG. **4**. The dialog **400** is illustrated as being displayed on the display **226** of the mobile communication device **100**.

As has been discussed above, the dialog **400** may include choices labeled "OK" and "Cancel". Furthermore, according to an aspect of the present disclosure, the dialog **400** may include another choice, labeled "Download Original".

It is expected that the user of the mobile communication device **100** will interact with the dialog **400** to select one of the choices. Accordingly, the signature handling application may receive (step **306**) an indication of the user selection and determine (step **308**) which of the choices the user has selected. Upon determining (step **308**) that the user has selected the "Cancel" choice, the signature handling application may return (step **310**) control to the message composition user interface.

Upon determining (step **308**) that the user has selected the "OK" choice, the signature handling application may generate (step **312**) a signature for the response message. To distinguish this signature from an alternative signature to be discussed hereinafter, this signature may be termed a "response" signature. The response signature is a result of encrypting a hash of the response message, where the response message includes the new portion, recently composed by the user of the mobile communication device **100**, and the initial portion of the first e-mail message (i.e., not the entire first e-mail message). The signature handling application may then arrange the transmission (step **314**) of the response message and the response signature.

Upon determining (step **308**) that the user has selected the "Download Original" choice, the signature handling application may obtain (step **316**) the remainder of the first e-mail message from the wireless mail server **118** and form (step **318**) a "new" message. The new message may be formed from the new portion, recently composed by the user of the mobile communication device **100**, and the entirety of the first e-mail message, obtained in step **316**. The signature handling application may then generate (step **320**) a signature for the new message. To distinguish this signature from the "response" signature, this signature may be termed a "new" signature. The new signature is a result of encrypting a hash of the new message. The signature handling application may then arrange the transmission (step **322**) of the new message and the new signature.

Additionally, the warning dialog **400** may include a checkbox labeled "Always download original". By selecting the checkbox labeled "Always download original" and then selecting the "Download Original" choice, the user may effectively set a policy for the mobile wireless device, where the policy indicates that all future signed, and/or encrypted, messages are to include the entirety of the original received message.

As a further alternative, the dialog **400** may include a checkbox labeled "Always send truncated" (not shown). By selecting the checkbox labeled "Always send truncated" (not shown) and then selecting the "OK" choice, the user may effectively set a policy for the mobile wireless device, where the policy indicates that all future signed, and/or encrypted, messages are to include only a truncated version of the original received message.

Apart from the dialog **400**, the user may be provided with an opportunity to establish a policy through editing a policy through use of a configuration options user interface. Such a configuration options user interface may allow the user to specify a size threshold for the original message so that an original message exceeding the size threshold is not automatically downloaded in its entirety for inclusion in the new message.

Notably, the automatic downloading of the original message may be accomplished on a background thread so that the user does not have to wait for the original message to be downloaded before carrying out further activities on the mobile communication device **100**. Responsive to indicating that the message is to be sent, the user may be prompted for a signing password, but the cryptographic key, for encrypting a hash of the new message, would not be used until after the original message has been downloaded.

Notably, the original message may not always be downloaded immediately. The mobile communication device **100** makes use of a data network connection to download the original message. Accordingly, in the absence of a data network connection, the mobile communication device **100** waits until a data network connection has been established, before downloading the original message.

The first cross-component message signing approach may be adapted for message encryption instead of, or in addition to, message signing. Steps of a method that is an example of adapting the first cross-component message signing approach to encryption are presented in FIG. **5**. Initially, the processor **228**, or, more accurately, an encryption handling application executed on the processor **228**, detects receipt (step **502**) of an instruction to transmit an encrypted response message. Such an instruction may be received from the message composition user interface application also executed on the processor **228**.

From the user's perspective, the user has specified that the response message is to be encrypted and the user has composed the new portion of the response message (in any order). The user may have configured the mobile communication device **100**, at some earlier time, to, by default, encrypt each outgoing messages. The receipt (detected in step **502**), by the encryption handling application, of the instruction to transmit an encrypted version of the response message may be triggered by the user opening a menu and selecting a "send" menu item.

Responsive to the detection in step **502**, the encryption handling application may present (step **504**) a dialog to warn the user that the first e-mail message will be incompletely included in the response message and giving the user choice regarding how or whether to proceed. An example of a suitable dialog is illustrated as a dialog **400** in FIG. **4**. The dialog **400** is illustrated as being displayed on the display **226** of the mobile communication device **100**.

As has been discussed above, the dialog **400** may include choices labeled "OK" and "Cancel". Furthermore, the dialog **400** may include another choice, labeled "Download Original".

It is expected that the user of the mobile communication device **100** will interact with the dialog **400** to select one of the choices. Accordingly, the encryption handling application may receive (step **506**) an indication of the user selec-

tion and determine (step **508**) which of the choices the user has selected. Upon determining (step **508**) that the user has selected the "Cancel" choice, the encryption handling application may return (step **510**) control to the message composition user interface.

Upon determining (step **508**) that the user has selected the "OK" choice, the encryption handling application may encrypt (step **512**) the response message. The encryption handling application may then arrange the transmission (step **514**) of the encrypted response message.

Upon determining (step **508**) that the user has selected the "Download Original" choice, the encryption handling application may obtain (step **516**) the remainder of the first e-mail message from the wireless mail server **118** and form (step **518**) a "new" message. The new message may be formed from the new portion, recently composed by the user of the mobile communication device **100**, and the entirety of the first e-mail message, obtained in step **516**. The encryption handling application may then encrypt (step **520**) the new message. The encryption handling application may then arrange the transmission (step **522**) of the encrypted new message.

A second cross-component message signing approach involves splitting the signing operation between the mobile communication device **100** and the wireless mail server **118**, thereby avoiding the downloading of the original message. Unlike the first approach, this split-signing approach cannot be considered to result in true end-to-end security, because the entire e-mail message is not signed strictly at the mobile communication device **100**. Rather, at least the new portion, recently composed by the user of the mobile communication device **100**, is signed strictly at the device, and the signing of the entire message, including the remainder not signed strictly at the device, involves the wireless mail server **118**. However, this second approach does provide a compromise between security and use of wireless channel resources, which makes it particularly suitable for signing large messages or messages with large attachments.

Steps of a method that is an example of the second approach are presented in FIG. **6**. Initially, the signature handling application detects receipt (step **602**) of an instruction to transmit a response message and an associated signature. Such an instruction may be received from the message composition user interface application also executed on the processor **228**.

Responsive to the detection in step **602**, the signature handling application may automatically add (step **603**) a disclaimer to the end of the response message, indicating that this point in the message marks the end of the part of the message signed at the mobile communication device **100** and/or the beginning of the part signed with the assistance of the wireless mail server **118**. For example, the disclaimer may be a line of text, such as "—end of device-signed data—". The signature handling application may further obtain (step **604**) a hash of the response message, where the response message includes the new portion, recently composed by the user of the mobile communication device **100**, and the initial portion of the first e-mail message (i.e., not the entire first e-mail message).

The signature handling application may then arrange the transmission (step **606**), to the wireless mail server **118**, of a request that the wireless mail server **118** continue the hashing across the first e-mail message. Along with the request, the signature handling application may arrange the transmission of the "context" of the hash of the response message to the wireless mail server **118**. The context may be an indication of the internal state of the hashing algorithm. Such an internal state indication may allow the wireless mail server **118** to continue to obtain the hash.

Steps in an example method of participating, at the wireless mail server **118**, in the split signing operation are illustrated in FIG. **7**. Initially, the wireless mail server **118** receives (step **702**) the hash continuation request. The wireless mail server **118** has awareness of the portion of the first e-mail message that was transmitted to the mobile communication device **100** and can therefore generate (step **704**) a "final" hash by hashing the portion of the first e-mail message that has not been transmitted to the mobile communication device **100**, where the final hash is a hash of a "new" message. The new message includes the new portion, recently composed by the user of the mobile communication device **100**, and the entirety of the first e-mail message.

Alternatively, if the hashing algorithm is a "streaming" algorithm, the mobile communication device **100** may transmit, to the wireless mail server **118**, the current value of the hash.

Upon completing generation (step **704**) of the hash across the first e-mail message, the wireless mail server **118** transmits (step **706**) the final hash to the mobile communication device **100**. It should be clear that the final hash is likely to be significantly smaller than the remainder of the original message.

Upon receiving (step **608**) the final hash from the wireless mail server **118**, the mobile communication device **100** signs (step **610**) the final hash and arranges (step **612**) the transmission of the response message and the encrypted hash to the wireless mail server **118**. The encrypted hash may be called the new signature.

Upon receiving (step **708**) the response message and the new signature, the wireless mail server **118** constructs the new message by appending (step **710**) the portion of the first e-mail message that has not been transmitted to the mobile communication device **100** to the response message and transmits (step **712**) the new message and the new signature.

Since the second cross-component message signing approach represented by the methods of FIGS. **6** and **7** may not be considered to result in true, end-to-end security, the user may be provided with an opportunity to select the second cross-component message signing approach on a per-message basis, depending on the size of the data and/or security requirements.

In a third cross-component message signing approach, the entire hash is generated on the wireless mail server **118**. The user composes the new portion and indicates that the response message and an associated signature are to be sent.

Steps of a method that is an example of the third cross-component message signing approach are presented in FIG. **8**. Initially, the signature handling application at the mobile communication device **100** detects receipt (step **802**) of an instruction to transmit the response message and the associated signature.

Responsive to the detection in step **802**, the signature handling application may arrange (step **804**) transmission of the new portion to the wireless mail server **118**.

Steps in an example method of participating, at the wireless mail server **118**, in the third cross-component message signing approach are illustrated in FIG. **9**. Initially, the wireless mail server **118** receives (step **902**) the new portion and appends the first e-mail message to the new portion, thereby forming (step **904**) the new message. The wireless mail server **118** then generates (step **906**) a hash of the new message. The wireless mail server **118** transmits (step **908**) the hash to the mobile communication device **100**.

At the mobile communication device **100**, the signature handling application receives (step **806**) the hash and signs (step **808**) the hash to generate the new signature. The signature handling application then arranges (step **810**) the transmission of the new signature to the wireless mail server **118**.

Upon receipt (step **910**) of the new signature, the wireless mail server **118** transmits (step **912**) the new message and the new signature.

The second approach to cross-component message signing exemplified in the combination of FIGS. **6** and **7** and the third approach to cross-component message signing exemplified in the combination of FIGS. **8** and **9** are suitable for message signing, but differences in the manner in which a message is signed and the manner in which a message is encrypted lead to a lack of direct applicability of these approaches to the encryption of a message.

In overview, the disclosed approaches for message signing may, with some adaptation, be extended for use in message encryption. In part, the adaptation involves the mobile communication device **100** transmitting additional, special cryptographic information to the wireless mail server **118**, thereby allowing the wireless mail server **118** to encrypt a given message.

FIG. **10** illustrates example steps of a cross-component message encryption approach. Initially, a message processing application executed on the processor **228** detects receipt (step **1002**) of an instruction to transmit an encrypted message. Such an instruction may be received from the message composition user interface application also executed on the processor **228**.

As discussed hereinbefore, where the message to be encrypted is a message that is formed from a new portion and an initial portion of an original message, the user of the mobile communication device **100** may prefer that the entirety of the original message be included as context for the new portion. However, as also discussed hereinbefore, only the initial portion of the original message may be present at the mobile communication device **100**. Furthermore, it is noted that the original message may have been encrypted.

Responsive to detecting receipt (step **1002**) of the instruction, the processor **228**, under control of the message processing application, may then obtain (step **1004**) the cryptographic information that the processor **228** would typically use to encrypt a message. Such cryptographic information may include, for example, one or more session keys, including a composite message session key for encrypting the composite message, along with one or more initialization vectors corresponding to each of the one or more session keys. An initialization vector is a block of bits that allows a stream cipher or a block cipher to be executed in any of several modes of operation to produce a unique stream independent from other streams produced by the same session key. Where the original message was encrypted, the cryptographic information may also include one or more session keys, such as an original message session key for decrypting the original message.

The processor **228**, under control of the message processing application, may then arrange the transmission (step **1006**), to the wireless mail server **118**, of the message whose transmission was requested in step **1002**. The message processing application may include, in the transmission, a request for the formation and encryption of a composite message along with the cryptographic information obtained in step **1004**.

FIG. **11** illustrates example steps in a method of participating, at the wireless mail server **118**, in the cross-component message encryption approach of FIG. **10**. Initially, the wireless mail server **118** receives (step **1102**) the new message, encryption request and associated cryptographic information.

In the case wherein the original message was encrypted, the wireless mail server **118** may then decrypt (step **1104**) the original message using an appropriate portion of the received cryptographic information.

The wireless mail server **118** may then create (step **1106**) a composite message by appending the original message to the new message. Both the new message and the original message may include a body portion and one or more attachments. Accordingly, while creating (step **1106**) the composite message, the wireless mail server **118** may append a body portion of the original message to a body portion of the new message and add attachments from the new message to the composite message and add attachments from the original message to the composite message.

Upon completing creation (step **1106**) of the composite message, the wireless mail server **118** encrypts (step **1108**) the composite message using an appropriate portion of the cryptographic information received in step **1102**. In conjunction with encrypting (step **1108**) the composite message, the wireless mail server **118** may wrap the composite message in an appropriate encoding. Such appropriate encoding may, for example, comprise encoding using a standard known as Secure/Multipurpose Internet Mail Extensions (S/MIME), which is a known standard for public key encryption and signing of data. Alternatively, such appropriate encoding may, for example, comprise encoding using a standard known as Pretty Good Privacy (PGP), which is a known data encryption and decryption computer standard that provides cryptographic privacy and authentication for data communication.

In an alternate implementation, rather than receiving the composite message session key from the mobile communication device **100**, the wireless mail server **118** generates the composite message session key and the corresponding initialization vector. This implementation may also involve sending the composite message session key to the mobile communication device **100**, so that the mobile communication device **100** may decrypt the sent composite message, if necessary.

When the composite message has been encrypted and wrapped, the wireless mail server **118** may transmit (step **1110**) the encrypted composite message toward recipients specified in a destination field of the new message.

FIG. **12** illustrates example steps of a cross-component message encryption approach distinct from the cross-component message encryption approach of FIGS. **10** and **11**. Initially, a message processing application executed on the processor **228** detects receipt (step **1202**) of an instruction to transmit an encrypted and signed message. Such an instruction may be received from the message composition user interface application also executed on the processor **228**.

As discussed hereinbefore, where the message to be encrypted and signed is a message that is formed from a new portion and an initial portion of an original message, the user of the mobile communication device **100** may prefer that the entirety of the original message be included as context for the new portion. However, as also discussed hereinbefore, often only the initial portion of the original message may be present at the mobile communication device **100**. Furthermore, it is noted that the original message may have been encrypted.

Responsive to detecting (step **1202**) receipt of the instruction, the processor **228**, under control of the message processing application, may then obtain (step **1204**) the cryptographic information that the processor **228** would typically use to encrypt a message. Such cryptographic information may include, for example, one or more session keys, including a composite message session key for encrypting the composite message, along with one or more initialization vectors corresponding to each of the one or more session keys. Where the original message was encrypted, the cryptographic information may also include one or more session keys, including an original message session key for decrypting the original message.

The processor **228**, under control of the message processing application, may then arrange the transmission (step **1206**), to the wireless mail server **118**, of the message whose transmission was requested in step **1002**. The message processing application may include, in the transmission, the cryptographic information obtained in step **1004** and a request for a hash of the composite message to be created, at the wireless mail server **118**, from the new message and the original message.

FIG. **13** illustrates example steps in a method of participating, at the wireless mail server **118**, in the cross-component message encryption approach of FIG. **12**. Initially, the wireless mail server **118** receives (step **1302**) the new message, associated cryptographic information and hash request.

In the case wherein the original message was encrypted, the wireless mail server **118** may then decrypt (step **1304**) the original message using an appropriate portion of the received cryptographic information.

The wireless mail server **118** may then create (step **1306**) a composite message by appending the original message to the new message. Both the new message and the original message may include a body portion and one or more attachments. Accordingly, while creating (step **1306**) the composite message, the wireless mail server **118** may append a body portion of the original message to a body portion of the new message and add attachments from the new message to the composite message and add attachments from the original message to the composite message.

Upon completing creation (step **1306**) of the composite message, the wireless mail server **118** generates (step **1308**) a hash of the composite message and transmits (step **1310**) the hash to the mobile communication device **100** with a hash signing request, specifying that the hash is to be signed.

Upon receiving (step **1208**) the hash signing request from the wireless mail server **118**, the mobile communication device **100** obtains (step **1210**) a private key specific to a user of the mobile communication device **100**. Obtaining (step **1210**) the private key may, for example, involve prompting the user for a password to allow the processor **228** access to a key store, in memory of the mobile communication device **100**, from which the processor **228** may obtain the private key.

Upon obtaining (step **1210**) the private key, the processor **228** may sign (step **1212**) the hash to form a signature for the composite message. The processor **228** may then arrange (step **1214**) the transmission of the signature to the wireless mail server **118**.

The wireless mail server **118** receives (step **1312**) the signature and adds (step **1314**) the signature to the composite message.

Upon adding (step **1314**) the signature to the composite message, the wireless mail server **118** may encrypt (step **1316**) the signed composite message using an appropriate portion of the cryptographic information received in step **1302**. In conjunction with encrypting (step **1316**) the signed composite message, the wireless mail server **118** may wrap the composite message in an appropriate encoding as discussed hereinbefore.

When the signed composite message has been encrypted and wrapped, the wireless mail server **118** may transmit (step **1318**) the encrypted and signed composite message toward recipients specified in a destination field of the new message.

The above-described embodiments of the present application are intended to be examples only. Alterations, modifications and variations may be effected to the particular embodiments by those skilled in the art without departing from the scope of the application, which is defined by the claims appended hereto.

What is claimed is:

1. At a mobile communication device, a method of processing an electronic message, said method comprising:
- receiving an initial part of an original message, said initial part of said original message having a size based on a size threshold in a policy established at a server associated with said mobile communication device;
- detecting receipt of an instruction to:
  - encrypt a composite message, where said composite message includes a new message related to said original message and an entirely of said original message; and
  - add a cryptographic signature to said composite message;
- obtaining a session key for use, at said server, in carrying out a request to encrypt said composite message;
- transmitting, to said server:
  - said new message; and
  - said request to encrypt said composite message, said request including:
    - said session key;
    - an indication of said original message; and
    - a request for a hash of said composite message;
- receiving, from said server, said hash;
- obtaining a private cryptographic key;
- employing said private cryptographic key to sign said hash, thereby forming a signed hash;
- transmitting, to said server, said signed hash thereby, allowing said server to use said signed hash to form a signed encrypted composite message for transmission; and
- providing, by the foregoing, maintenance of security considerations in view of bandwidth optimization measures.

2. The method of claim **1** wherein said session key for use in carrying out said request to encrypt said composite message comprises a composite message session key.

3. The method of claim **2** wherein said request to encrypt said composite message further comprises an initialization vector corresponding to said session key.

4. The method of claim **1** wherein said session key for use in carrying out said request to encrypt said composite message comprises an original message session key.

5. A mobile communication device comprising a processor adapted to:
- receive an initial part of an original message, said initial part of said original message having a size based on a size threshold in a policy established at a server associated with said mobile communication device;

detect receipt of an instruction to:
encrypt a composite message, where said composite message includes a new message related to said original message and an entirely of said original message; and
add a cryptographic signature to said composite message;
obtain a session key for use, at said server, in carrying out a request to encrypt said composite message;
arrange transmission, to said server, of:
said new message; and
said request to encrypt said composite message, the request including:
said session key;
an indication of said original message; and
a request for a hash of said composite message;
receive, from said server, said hash;
obtain a private cryptographic key;
employ said private cryptographic key to sign said hash, thereby forming a signed hash;
transmit, to said server, said signed hash, thereby allowing said server to use said signed hash to form a signed encrypted composite message for transmission; and
provide, by the foregoing, maintenance of security considerations in view of bandwidth optimization measures.

6. The mobile communication device of claim **5** wherein said session key for use in carrying out said request to encrypt said composite message comprises a composite message session key.

7. The mobile communication device claim **6** wherein said request to encrypt said composite message further comprises an initialization vector corresponding to said session key.

8. The mobile communication device of claim **5** wherein said session key for use in carrying out said request to encrypt said composite message comprises an original message session key.

9. A non-transitory computer-readable medium containing computer-executable instructions that, when performed by a processor in a mobile communication device, cause said processor to:
receive an initial part of an original message, said initial part of said original message having a size based on a size threshold in a policy established at a server associated with said mobile communication device;
detect receipt of an instruction to:
encrypt a composite message, where said composite message includes a new message related to said original message and an entirely of said original message; and
add a cryptographic signature to said composite message;
obtain a session key for use, at said server, in carrying out a request to encrypt said composite message;
arrange transmission, to said server:
said new message; and
said request to encrypt said composite message, the request including:
said session key;
an indication of said original message; and
a request for a hash of said composite message;
receive, from said server, said hash;
obtain a private cryptographic key;
employ said private cryptographic key to sign said hash, thereby forming a signed hash;
transmit, to said server, said signed hash thereby, allowing said server to use said signed hash to form a signed encrypted composite message for transmission; and
provide, by the foregoing, maintenance of security considerations in view of bandwidth optimization measures.

10. The non-transitory computer-readable medium of claim **9** wherein said session key for use in carrying out said request to encrypt said composite message comprises a composite message session key.

11. The non-transitory computer-readable medium of claim **10** wherein said request to encrypt said composite message further comprises an initialization vector corresponding to said session key.

12. The non-transitory computer-readable medium of claim **9** wherein said session key for use in carrying out said request to encrypt said composite message comprises an original message session key.

13. At a mail server having a processor, said server associated with a mobile communication device, a method of processing an electronic message, said method comprising:
splitting an entire original message into an initial part and a remaining part, said initial part having a size based on a size threshold in a policy established at said server;
transmitting, to said mobile communication device, said initial part;
detecting, by said processor, receipt, from said mobile communication device, of a message processing request for encryption of a composite message, where said composite message includes a new message related to said original message and said entire original message, said message processing request including:
said new message;
a session key for use in said encryption; and
a request to sign said composite message;
creating, by said processor, said composite message from said new message and said entire original message;
employing said session key to encrypt, by said processor, said composite message to form an encrypted composite message;
generating a hash of said composite message;
transmitting, to said mobile communication device, said hash;
receiving a signature, where said signature comprises said hash signed at said mobile communication device using a private key;
adding said signature to said composite message, thereby forming a signed encrypted composite message;
transmitting, via a communication subsystem, said signed encrypted composite message; and
providing, by the foregoing, maintenance of security considerations in view of bandwidth optimization measures.

14. The method of claim **13** wherein said session key is a composite message session key and the method further comprising employing an original message session key to decrypt said original message prior to said creating of said composite message.

15. The method of claim **13** wherein said creating said composite message comprises including an attachment received in association with said new message.

16. The method of claim **13** wherein said creating said composite message comprises including an attachment received in association with said original message.

17. A mail server associated with a mobile communication device, said mail server comprising a processor adapted to:

split an entire original message into an initial part and a remaining part, said initial part having a size based on a size threshold in a policy established at said server;

transmit, to said mobile communication device, said initial part;

detect receipt, from said mobile communication device, of a message processing request for encryption of a composite message, where said composite message includes a new message related to said original message and said entire original message, said message processing request including:

said new message;

a session key for use in said encryption; and

a request to sign said composite message;

create said composite message from said new message and said entire original message;

employ said session key to encrypt said composite message to form an encrypted composite message;

generate a hash of said composite message;

transmit, to said mobile communication device, said hash;

receive a signature, where said signature comprises said hash signed at said mobile communication device using a private key;

add said signature to said composite message, thereby forming a signed encrypted composite message;

arrange transmission of said signed encrypted composite message; and

provide, by the foregoing, maintenance of security considerations in view of bandwidth optimization measures.

18. The mail server of claim 17 wherein said session key is a composite message session key and said processor is further adapted to employ an original message session key to decrypt said original message prior to said creating of said composite message.

19. The mail server of claim 17 wherein said processor is further adapted to create said composite message by including an attachment received in association with said new message.

20. The mail server of claim 17 wherein said processor is further adapted to create said composite message by including an attachment received in association with said original message.

21. A non-transitory computer-readable medium containing computer-executable instructions that, when performed by a mail server associated with a mobile communication device, said mail server including a processor, said instructions causing said processor to:

split an entire original message into an initial part and a remaining part, said initial part having a size based on a size threshold in a policy established at said server;

transmit, to said mobile communication device, said initial part;

detect receipt, from said mobile communication device, of a message processing request for encryption and transmission of a composite message, where said composite message includes a new message related to said original message and original message, said message processing request including:

said new message;

a session key for use in said encryption; and

a request to sign said composite message;

create said composite message from said new message and said entire original message;

employing said session key to encrypt said composite message to form an encrypted composite message;

generate a hash of said composite message;

transmit, to said mobile communication device, said hash;

receive a signature, where said signature comprises said hash signed at said mobile communication device using a private key;

add said signature to said composite message, thereby forming a signed encrypted composite message;

arrange transmission of said signed encrypted composite message; and

provide, by the foregoing, maintenance of security considerations in view of bandwidth optimization measures.

22. The non-transitory computer-readable medium of claim 21 wherein said session key is a composite message session key and the instructions further cause said processor to employ an original message session key to decrypt said original message prior to said creating of said composite message.

23. The non-transitory computer-readable medium of claim 21 wherein said instructions further cause said processor to create said composite message by including an attachment received in association with said new message.

24. The non-transitory computer-readable medium of claim 21 wherein said instructions further cause said processor to create said composite message by including an attachment received in association with said original message.

* * * * *